

National Payments Corporation of India (NPCI)

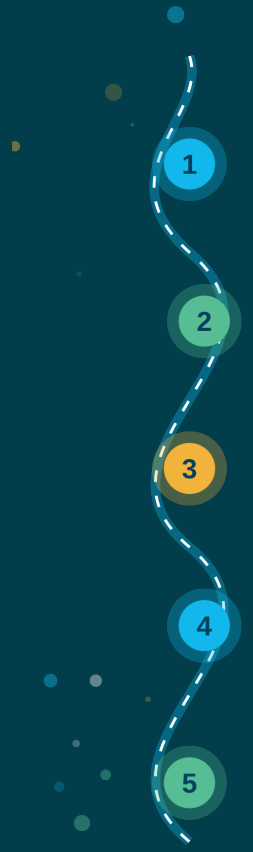
UPI & RuPay – Product Overview & Security Standards

Swapnil Kulkarni

Sr. Lead – Governance, Risk & Compliance

Agenda

1. About NPCI and its Products: UPI and RuPay
2. Business Growth & the Compliance Challenge
3. NPCI's Security Frameworks: Domains and Technical Controls
4. Alignment with PCI and International Standards
5. Shared Responsibility Across the Ecosystem



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

About NPCI and UPI Ecosystem



NPCI – Network for India's Retail Payment Rails

Not-for-profit initiative of the Reserve Bank of India (RBI) and the Indian Banks' Association

UPI
Real-time payments

RuPay
Card network

IMPS
Instant transfers

AePS
Aadhaar payments

Bharat Connect
Bill payments

NETC
FASTag tolls

NACH
Mandates

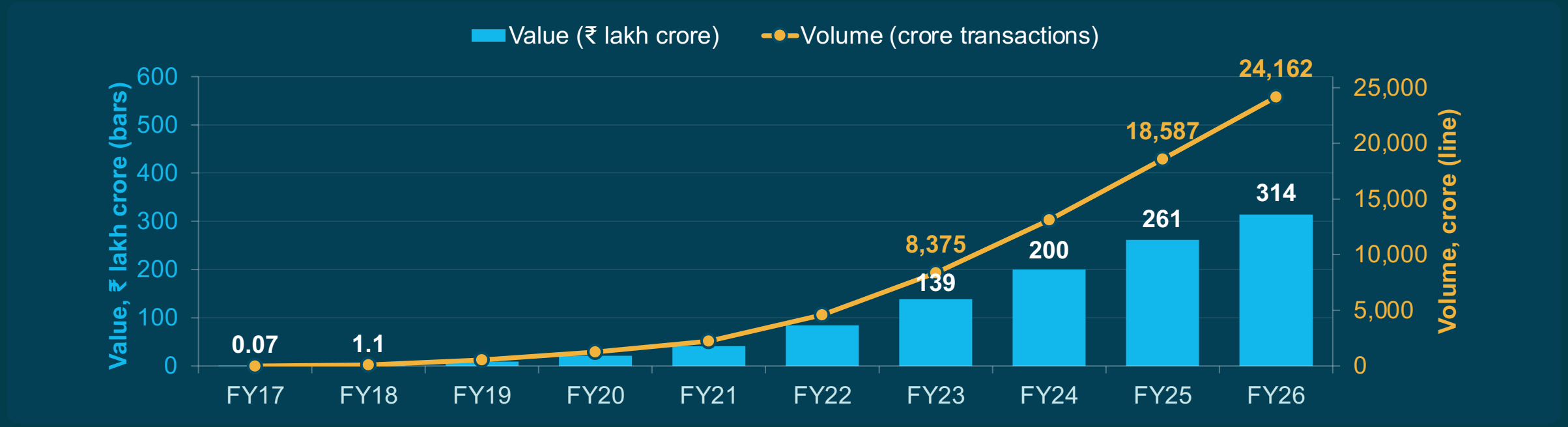
CTS
Cheque truncation



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

UPI Growth: A Decade of Scale

Annual value (bars) and volume (line), FY17 to FY26



~13,500x	growth in volume, FY17 to FY26
~4,500x	growth in value, FY17 to FY26
₹314 lakh cr	value in FY26 (≈ US$3.5 trillion)

Source: NPCI UPI Product Statistics. FY = April–March.

20 YEARS OF SECURING PAYMENT DATA

UPI – Real-time, 24×7×365, fully interoperable

Numbers at a glance

802 mn
transactions per day (average, Sep 2026)

24.07 bn
transactions in a month (Sep 2026)

₹29.37 lakh Cr.
value in a month (≈ US$330 bn, Sep 2026)

750+
banks live on UPI

11
countries with UPI acceptance



Source: NPCI UPI product statistics, September 2026.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Key Participants in UPI: PSP, TPAP and ASP

Clear roles, clear security accountability

Customer | TPAP app | Sponsor PSP bank | NPCI UPI switch | Customer's bank

PSP Banks
Payment Service Provider

A bank authorized to connect directly to the UPI switch

- Onboards customers and issues UPI IDs
- Sponsors third-party apps and is accountable for them
- Owns fraud monitoring, risk and compliance

TPAP
Third-Party Application Provider

A non-bank UPI app offered to consumers

- Connects only through sponsor PSP bank(s)
- Meets NPCI app-security and data requirements
- Audited at onboarding and periodically

ASP
Application Service Provider

A technology partner that builds or runs UPI systems for a bank

- Operates under the bank's control and contract
- Covered by NPCI frameworks and third-party risk controls
- Same security bar as the bank it serves

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

UPI Transaction Flow

UPI QR P2M (Person-to-Merchant) financial transaction



1. Payment request
Customer scans the merchant QR and authorizes with UPI PIN

2. Payer PSP bank
Validates the request and forwards it to the NPCI UPI switch

3. Payee PSP bank
NPCI validates the merchant and maps its UPI ID to the account

4. Remitter bank
Verifies the PIN and debits the customer's account

5. Beneficiary bank
Credits the merchant's account

6. Confirmation
Customer and merchant are notified, typically within seconds

The UPI PIN is encrypted on the device, only the customer's own bank can verify it.

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

How UPI Stays Safe and Secure

Built into the rails, required of every participant, supported by NPCI

Checks on Every Payment

- Device bound to SIM and phone
- Two factors: device + UPI PIN
- PIN encrypted: never visible to apps
- Signed, encrypted messages
- Real-time risk scoring and limits

What Participants Must Meet

- NPCI security and mobile-app frameworks
- Independent annual audits
- Self-attestation with evidence
- Incident reporting within 6 hours
- Time-bound closure of findings

Participants' Own Monitoring

- 24×7 SOC
- Fraud monitoring through EFRM (Enterprise Fraud Risk Management)
- Regular VAPT
- App and API security testing

How NPCI Supports

- Threat intelligence and advisories
- Central fraud signals and blocking
- Incident coordination with CERT-In and RBI
- Compliance tracking and oversight

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

Security Built into Every UPI Transaction

Device Binding
SMS from registered SIM

Two Factors
Bound device + UPI PIN

PIN Hidden from Apps
Encrypted in NPCI Common Library

HSM-Only Decryption
Signed messages, secured channels

No Account Numbers
Virtual payment addresses

Network Risk Scoring
Real-time, limits, cooling periods



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

UPI Device Binding

Hardening the root of trust for every UPI account



Pre-checks

Latest app version



Dynamic Token

Alphanumeric and

Timebound



Outbound SMS

Register mobile number of customer in bank records

Delivery receipt first



One Session

App switch voids token

One device only



Verify & Alert

Auto-read OTP only

SMS alerts to user

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

UPI Security Measures: Prevent, Detect, Educate

Controls for users, banks and the wider ecosystem

Authenticate & Onboard

- Two-factor: mobile number bound to the device, plus UPI PIN
- UPI PIN set using Aadhaar or debit-card credentials
- Cooling period limits transactions after a new registration

Detect & Limit

- AI / ML (Artificial Intelligence / Machine Learning) models decline suspicious transactions
- Daily limits by transaction type, on debit and credit sides
- FRM (Fraud Risk Management) tool for all banks to set rules, alert or decline

Inform & Educate

- In-app alert when paying an unknown beneficiary
- Beneficiary name shown from the bank's CBS (Core Banking System); PIN page states the account will be debited
- Regular training for banks and PSPs
- Customer awareness on digital media, radio and TV

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

How NPCI Engages the Ecosystem

A continuous two-way loop between NPCI and banks, PSPs and TPAPs



20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

We meet the Bar Before we set it

NPCI's own infrastructure

PCI DSS, SSF, PIN : annual QSA assessment

ISO/IEC 27001, 42001, 22301, 27701

Programme built on NIST CSF 2.0

24×7 SOC, Red teaming, Breach-and-attack simulation

Quarterly and surprise DR drills

Cyber Strategy – Defence in Depth

How NPCI protects its own critical information infrastructure

Layered Approach

- Multiple layers that complement each other
- Resilient systems with compensating controls

Perimeter DDoS protection · Honeypots · VPN gateways

Network IDS/IPS · Firewalls · Segmentation · Proxy

Application WAF · API security

Access NAC · 2FA · Tokenization

Endpoint HIPS · Antivirus · APT · FIM

Data DLP · IRM/DRM · Encryption

Monitoring SIEM · UEBA

Response MDR · SOAR

Critical Information Infrastructure

Multi-Vendor Environment

- Diverse vendors strengthen the architecture
- Protection across assets, identities and information

DDoS: Distributed Denial of Service · IDS/IPS: Intrusion Detection/Prevention System · WAF: Web Application Firewall · NAC: Network Access Control · 2FA: Two-Factor Authentication · HIPS: Host Intrusion Prevention System · APT: Advanced Persistent Threat protection · FIM: File Integrity Monitoring · DLP: Data Loss Prevention · IRM/DRM: Information/Digital Rights Management · SIEM: Security Information and Event Management · UEBA: User and Entity Behaviour Analytics · MDR: Managed Detection and Response · SOAR: Security Orchestration, Automation and Response

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

The Compliance Challenge



Why the Ecosystem Needs a Common Baseline

Different entity types, frameworks and submission cycles

Entity	Key obligations	Submission rhythm
UPI PSPs, ASPs (Application Service Providers), TPAPs (Third Party Application Providers)	UPI InfoSec Framework, Mobile App Security Framework	Annual CERT-In audit
Issuer & acquirer banks	RuPay framework, PCI DSS / PIN / PTS, RBI IT directions	PCI cycle, product ccertifications, monthly fraud reports
PPI (Prepaid Payment Instruments) issuers	RBI PPI and cyber resilience directions	RBI audit cycle plus NPCI submissions
Payment Gateway and Aggregators, token requestors	RBI PA directions, tokenization rules, PCI Compliance	Quarterly, annual and monthly reports

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

NPCI Security Frameworks and Circulars

One security bar for every participant on every rail



NPCI Security Frameworks at a Glance

Issued by NPCI as the network operator

UPI Information Security Compliance Framework
Security baseline for banks, PSPs, TPAPs and ASPs on UPI

Mobile Application Security Framework for UPI
Mandatory app protections; independent audit at onboarding and annually

RuPay Information Security Compliance Framework
Security expectations for RuPay issuers, acquirers and processors

Cyber Incident Reporting Circular
Cyber incidents reported to NPCI within 6 hours

Threat and Ransomware Advisories
Timely, actionable guidance as threats emerge

Device Binding and Risk Management Circulars
Stronger customer onboarding and fraud controls

18+	security domains
25+	global and Indian reference standards
40+	circulars and advisories

20 YEARS OF SECURING PAYMENT DATA

Security Domains Covered by NPCI Frameworks

Key Focus Areas

- **Identity & Access Management**
- **Network Security**
- **Application Security**
- **Data Security & Cryptography**
- **Cloud Security**
- **Third-Party Risk Management**
- **Security Operations & Incident Response**
- **Fraud Risk Management**
- **AI & Emerging Technology**
- **Security Assessment & VAPT**
- **Mobile Application Security**
- **API Security**

Foundational Governance & Resilience

- Governance, Risk & Compliance
- Asset Management
- Data Privacy & Protection
- Human Resource Security
- Physical & Environmental Security
- System Security & Vulnerability Management
- Business Continuity & Disaster Recovery
- Forensics & Legal Assurance
- Operations Management

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Security Operations · Security Testing

Security Operations

24×7 SOC (Security Operations Centre)
Continuous monitoring with defined detection and response timelines

Forensic-Ready Logs
Long-term log retention; SIEM (Security Information and Event Management) and EDR (Endpoint Detection and Response)

6-Hour Reporting
To CERT-In (Indian Computer Emergency Response Team), RBI and NPCI

Assessment & VAPT

Risk-Based Cadence
Periodic independent VAPT (Vulnerability Assessment & Penetration Testing), internal and external

Apps and APIs
Tested periodically and before every major release

Red Teaming
Adversary simulation; time-bound closure of findings

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Identity & Access · Network Security

Identity & Access

Privileged Access Management (PAM)
Controlled, time-bound and recorded administrator access

Strong MFA (Multi-Factor Authentication)
For remote, privileged and sensitive access, no SMS OTP (One-Time Password) for administrators

Identity Lifecycle
Automated joiner-mover-leaver, segregation of duties (maker is never checker)

Network Security

Application-Layer (Layer 7) Default Deny
Every firewall rule justified, approved and reviewed periodically

Segmentation & Zero Trust
Segmented internal traffic, layered DMZ (Demilitarized Zone)

Isolated Payment Core
No direct internet path to switches, databases or HSMs (Hardware Security Modules)

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Cryptography · Cloud Security

Data Security & Cryptography

Encryption Everywhere
AES at rest, TLS and mutual TLS in transit

HSM Key Lifecycle
Governed key ceremonies, rotation on custodian change

PIN & Token Security
PIN encrypted at entry, TR-31 (ANSI X9 key-block) key protection; unique tokens

Cloud Security

Isolated Landing Zone
Separate production, development, logging and security environments

Residency by Policy
Data stays in approved regions, enforced by policy

Customer-Held Keys
BYOK/HYOK (Bring / Hold Your Own Key), CSPM (Cloud Security Posture Management)

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Application Security · API Security

Application Security

Secure by Design
Threat modelling (STRIDE*), SAST, SBOM

Runtime Protection
WAF in blocking mode; strict input validation

Payment Software
Built to the PCI Secure Software Framework (SSF)

API Security

Know Every API
Complete inventory, including undocumented (shadow) APIs

Object-Level Authorization
Checked on every request: BOLA / BFLA (Broken Object / Function Level Authorization)

Gateway Enforcement
mTLS, rate limits and schema validation

*STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Mobile App Security · Fraud Risk

Mobile App Security

Device Trust
Detects rooted devices, emulators and unofficial install sources

Anti-Takeover
Blocks misuse of accessibility services and screen mirroring

Runtime Shielding
Code obfuscation, anti-tampering, anti-instrumentation, certificate pinning

Fraud Risk Management

Real-Time Screening
Every transaction risk-scored before authorization

Adaptive Friction
Step-up authentication; cooling period after sensitive changes

Rapid Response
Money-mule detection, central blocking, customer self-block

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

AI & Emerging Tech · Third-Party Risk

AI & Emerging Tech

AI Governance
ISO/IEC 42001 and NIST AI RMF (Risk Management Framework), AI inventory

Adversarial Defence
Guardrails against prompt injection, AI outputs treated as untrusted

Human Oversight
Human in the loop for high-risk decisions

Third-Party Risk

Single Register
Every outsourced arrangement, tiered by criticality

Audit Rights
For the entity, NPCI and the regulator

Supply-Chain Depth
Fourth- and nth-party mapping, certified data destruction

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Value and Alignment

Why a Common Baseline Works



20 YEARS OF SECURING PAYMENT DATA

PCI Security Standards Council

What a Unified Baseline Delivers

Harmonised

One baseline for every rail

Integrated

Security and privacy together

Mapped

Comply once, show many times

Assurable

Consistent audit conclusions

Proportionate

Scaled to role and data

Adaptive

Cloud, API, mobile and AI ready

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Aligned with PCI and International Standards

NPCI frameworks are aligned with PCI and international standards

PCI Security Standards

PCI DSS v4.0.1

PCI PIN Security

PCI Secure Software Framework

PCI P2PE and PTS terminals

PCI Card Production

ISO/IEC	27001 · 27701 · 27017 · 42001
NIST	CSF 2.0 · SP 800-53 · 800-207
Industry	CIS · OWASP · CSA CCM
India	RBI · CERT-In · DPDP Act · UIDAI

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

What NPCI Frameworks Add Alongside PCI

For an account-to-account, multi-rail ecosystem

- Privacy (DPDP Act)
- Consumer Mobile Apps
- Fraud Risk Management
- AI & Emerging Tech
- Resilience & DR
- Forensics & Legal
- API Security
- Indian Regulatory Layer
- Rail-Specific Mandates

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Thank You



20 YEARS OF SECURING PAYMENT DATA